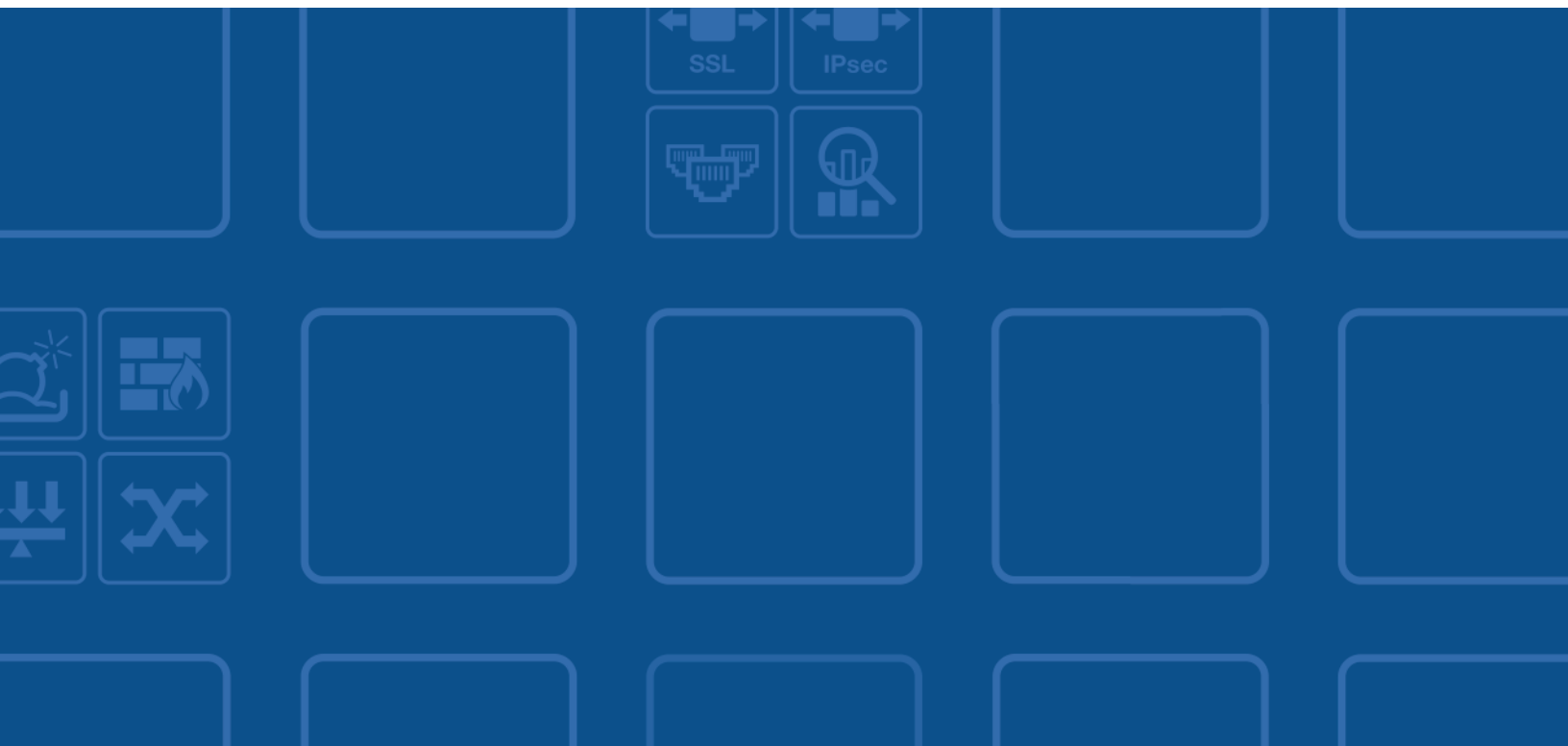
FORTINET
High Performance Network Security

FortiClient EMS for Chromebooks - QuickStart Guide

VERSION 1.0.3



FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

January 10, 2017

FortiClient Enterprise Management Server for Chromebooks 1.0.3 QuickStart Guide

04-103-381624-20170110

TABLE OF CONTENTS

Change Log

Date	Change Description
2016-11-18	Initial release of 1.0.3.
2016-11-29	Update to clarify how to add Service Account Credentials.
2017-01-10	Updated example for configuring the FortiClient Web Filter extension.

Introduction

This guide describes how to install and set up FortiClient Enterprise Management Server (EMS) for Chromebooks. It also describes how to set up Google Admin console to use the FortiClient Web Filter extension. Together the products provide web filtering for Google Chromebook users.

Supported installation platforms

You can install FortiClient EMS for Chromebooks on the following platforms:

- Microsoft Windows Server 2012, 2012 R2
- Microsoft Windows Server 2008 R2

For information about minimum system requirements and the latest information about supported platforms, see the *FortiClient EMS for Chromebooks Release Notes*, available in the Fortinet Document Library.

Requirements

The following components and knowledge are required to use FortiClient EMS for Chromebooks:

- FortiClient EMS for Chromebooks installer
- FortiClient Web Filter extension available in the Google Web Store for Chrome OS
- Google For Work account
- Knowledge of administering the Google Admin console
- A domain configured in Google Admin console
- SSL certificate to support communication between FortiClient Web Filter extension and FortiClient EMS for Chromebooks
- SSL certificate to support communication between FortiClient Web Filter extension and FortiAnalyzer for logging, if using
- Unique set of Service Account Credentials

Required services and ports

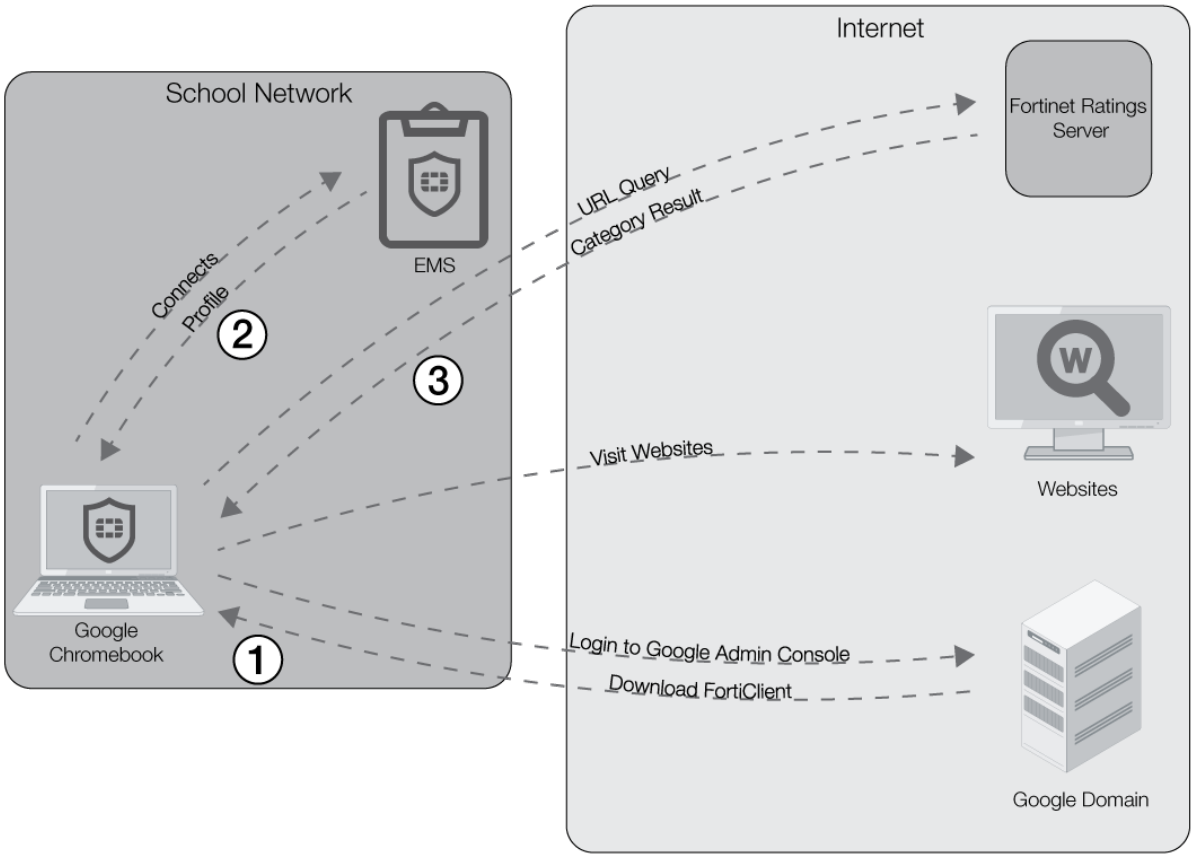
You must ensure that required ports and services are enabled on the server for use by FortiClient Enterprise Management Server for Chromebooks and its associated applications. The required ports and services enable FortiClient Enterprise Management Server for Chromebooks to communicate with clients and servers running associated applications.

Communication	Service	Protocol	Port
Apache	HTTPS	TCP	443
SQL server			
FortiClient on Chrome OS • Connection to Profile Server.			8443 (default) You can customize this port.

How the products work together

After you install and configure FortiClient EMS for Chromebooks, Google Admin Console, and the FortiClient Web Filter extension, the products work together to provide web-filtering security for Google Chromebook users that are logged into the Google domain. Following is a summary of how the products work together after the setup is complete:

1. When Google Chromebook users log into Google Chromebook, Google Chromebook downloads the FortiClient Web Filter extension.
2. FortiClient connects to FortiClient EMS for Chromebooks, and downloads a profile to Google Chromebook. The profile contains the web-filtering settings from FortiClient EMS for Chromebooks.
3. When Google Chromebook users browse the Internet, FortiClient sends the URL query to the Fortinet Ratings Server, and the Fortinet Ratings server returns the category result to FortiClient. FortiClient compares the category results with the profile to determine whether to allow the Google Chromebook user to access the URL.


Internet
School Network
Fortinet Ratings Server
EMS
URL Query
Category Result
Connects
Profile
2
3
Visit Websites
Websites
Google Chromebook
1
Login to Google Admin Console
Download FortiClient
Google Domain

Installation

Following is a summary of how to install and start FortiClient EMS for Chromebooks:

1. Download the installation file. See Downloading the installation file on page 9.
2. Install FortiClient EMS for Chromebooks. See Installing FortiClient EMS on page 9.
3. Start FortiClient EMS for Chromebooks. See Starting FortiClient EMS on page 10.

Downloading the installation file

FortiClient EMS for Chromebooks is available for download from the following locations:

- Fortinet Support website: https://support.fortinet.com/
- Sales representative

The following installation file is available for FortiClient EMS for Chromebooks:

- `FortiClientEnterpriseManagement_Chromebook_1.0.3.<build>_x64.exe`

For more information about obtaining FortiClient EMS for Chromebooks, contact your Fortinet reseller.

Installing FortiClient EMS

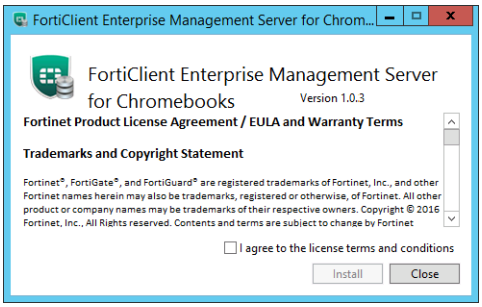
The FortiClient EMS for Chromebooks installation package includes:

- FortiClient EMS for Chromebooks
- Microsoft SQL Server 2014 Express Edition
- Apache HTTP server

Local administrator rights and Internet access are required to install FortiClient EMS for Chromebooks.

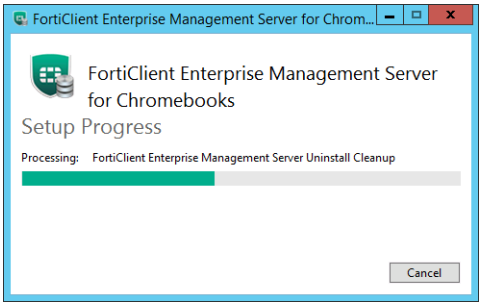
To install FortiClient EMS for Chromebooks:

1. If you are logged into the system as an administrator, double-click the downloaded installation file.
   If you are not logged in as an administrator, right-click on the installation file, and select *Run as administrator* from the pop-up menu.
2. If applicable, select *Yes* in the *User Account Control* window to allow the program to make changes to your system.
3. In the installation window, select *I agree to the license terms and conditions*, if you agree with the license terms and conditions. If you do not agree, you cannot install the software.

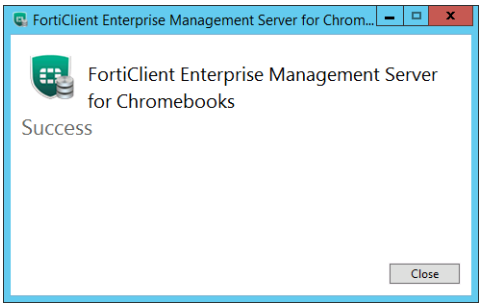


4. Select *Install*.

   The installation may take 30 minutes or longer. It may appear to stop at times, but this is only because certain steps in the installation process take longer than others. Please be patient.



5. When the program has installed correctly, the *Success* window will be displayed. Select *Close* to close the window.



   A *FortiClient Enterprise Management Server* icon will be added to the desktop.

Starting FortiClient EMS

To start FortiClient EMS:

1. Double-click the *FortiClient Enterprise Management Server* icon to start FortiClient EMS.
2. Sign in with username *admin* and no password.
3. Change the username and password by going to *View* > *User Management* > *Administration*.
4. Configure the endpoint server and client settings, including the IP address that FortiClient EMS will listen on, by going to *View* > *Settings*.

Accessing FortiClient EMS remotely

You can access FortiClient EMS for Chromebooks remotely by using a web browser instead of the GUI.

To enable remote access to FortiClient EMS for Chromebooks:

1. Go to *View* > *Settings*.
2. On the *Server Settings* tab, enable *Remote Administration HTTPS Access*.
3. Select *Save*.

To remotely access FortiClient EMS for Chromebooks:

- To access EMS from the EMS server, visit `https://localhost`
- To access the server remotely, use the server's hostname: `https://<server_name>`

  Ensure that you can ping `<server_name>` remotely. This can be achieved by adding it into a DNS entry or by adding it to the Windows hosts file. You may have to modify the Windows firewall rules to allow the connection.

Google Admin Console Setup

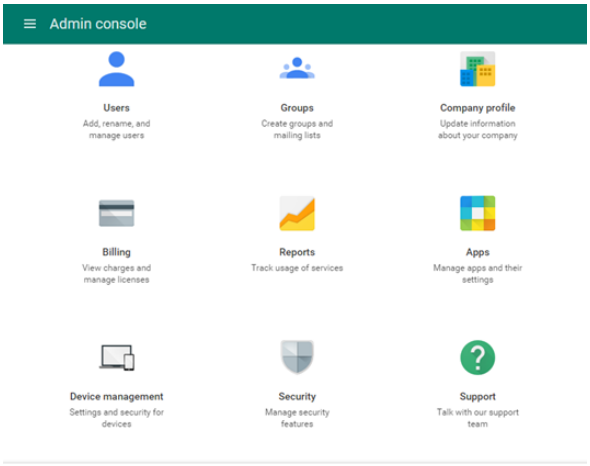
This section describes how to set up Google Admin console. Following is a summary of how to set up Google Admin console:

1. Log into Google Admin console. See Logging into Google Admin console on page 12
2. Add the FortiClient Web Filter extension. See Adding the FortiClient Web Filter extension on page 12.
3. Configure the FortiClient Web Filter extension. See Configuring the FortiClient Web Filter extension on page 13.
4. Add the root certificate. See Adding root certificates on page 14.
5. Disallow incognito mode. See Disallowing incognito mode on page 16

Logging into Google Admin console

To log into Google Admin console:

1. Log into Google Admin console (https://admin.google.com) by using your Google Domain admin account. The Admin console is displayed.



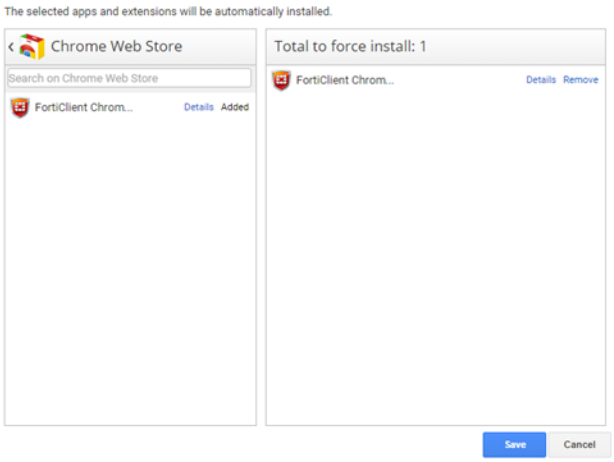
Adding the FortiClient Web Filter extension

The FortiClient Web Filter extension is available in the Google Web Store for Chrome OS.

FortiClient EMS for Chromebooks software is not available for public use. You can only enable the feature by using the following extension ID: igbg-pehnbmhgdgjbhkkpedommgmfbeao

To add the FortiClient Web Filter extension:

1. In Google Admin console, go to *Device management* > *Chrome Management* > *User Settings* > *Apps and Extensions* > *Force-installed Apps and Extensions* > *Manage force-installed apps*.
2. Select *Chrome Web Store*, and search for the following extension ID: igbgpehnbmhgdgjbhkkpedommgmfbeao
3. Add the extension ID and save.
   The extension name is displayed as *FortiClient Chromebook Web Filter Extension*.



Configuring the FortiClient Web Filter extension

You must configure the FortiClient Chromebook Web Filter extension to enable Google Admin console to communicate with FortiClient EMS for Chromebooks.

FortiClient EMS for Chromebooks hosts the services that assign endpoint profiles of web-filtering policies to groups in the Google domain. FortiClient EMS for Chromebooks also handles the logs and web-access statistics sent from the FortiClient Web Filter extensions.

FortiClient EMS for Chromebooks is the profile server.

To configure the FortiClient Web Filter extension:

1. In FortiClient EMS for Chromebooks, locate the server name and port by going to *View* > *Settings* > *EMS for Chromebook*.
2. Create a text file that contains the following text:

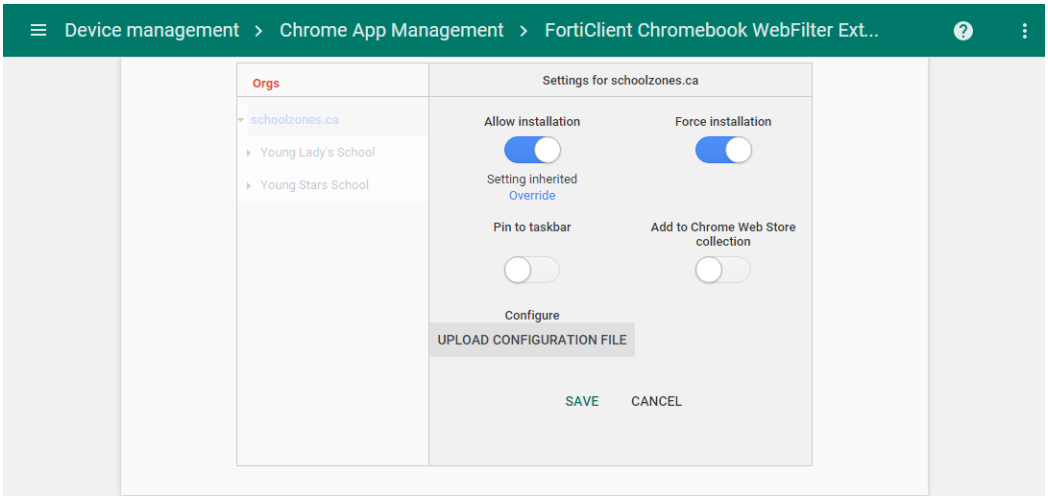
```
{
   "ProfileServerUrl": { "Value": "https://< ProfileServer >:< port for Profile Server >"}
}
```

   For example:

```
{
   "ProfileServerUrl": { "Value": "https://ems.mydomain.com:8443"}
}
```

3. In Google Admin console, go to *Device management* > *Chrome Management* > *App Management* > *FortiClient Chrome Web Filter Extension* > *User settings*.

4. Click a domain or organization unit (OU).
5. In the right pane, under *Configure*, upload a new configure file.
   You can also view the current setting.



6. Click *Save*.

Adding root certificates

This section includes the following information:

About communication with FortiClient Web Filter extension

The FortiClient Chromebook Web Filter extension communicates with FortiClient EMS for Chromebooks by using HTTPS connections. The HTTPS connections require an SSL certificate. You must obtain an SSL certificate and add the certificate to FortiClient EMS for Chromebooks to allow the FortiClient Web Filter extension to trust FortiClient EMS for Chromebooks.

If you use a public SSL certificate, you only need to add the public SSL certificate to FortiClient EMS for Chromebooks. See Adding SSL certificates on page 20.

However, if you prefer to use a certificate that is not from a common CA, you must add the SSL certificate to FortiClient EMS for Chromebooks, and you must also push the root CA of your certificate to the Google Chromebooks. Otherwise, the HTTPS connection between the FortiClient Chromebook Web Filter extension and FortiClient EMS for Chromebooks will not work. See Adding root certificates to Google Admin console on page 15.

About communication with FortiAnalyzer for logging

FortiClient EMS for Chromebooks supports logging to FortiAnalyzer. If you have a FortiAnalyzer device and configure FortiClient EMS for Chromebooks to send logs to FortiAnalyzer, an SSL certificate is required to

support communication between FortiClient Web Filter extension and FortiAnalyzer.

If you use a public SSL certificate, you only need to add the public certificate to FortiAnalyzer. See Adding SSL certificates to FortiAnalyzer on page 20.

However, if you prefer to use a certificate that is not from a common CA, you must add the SSL certificate to FortiAnalyzer, and you must also push the root CA of your certificate to the Google Chromebooks. Otherwise, the HTTPS connection between the FortiClient Chromebook Web Filter extension and FortiAnalyzer will not work. See Adding root certificates to Google Admin console on page 15.

The following table summarizes where to add certificates for each scenario:

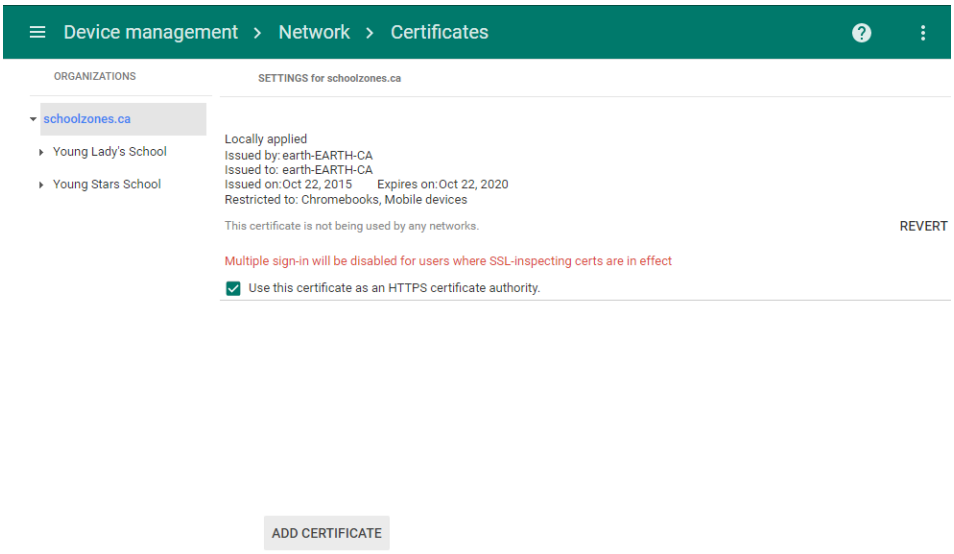
Scenario	Certificate and CA	Where to Add Certificates
Allow FortiClient Chromebook Web Filter extension to trust EMS	Public SSL certificate	• Add SSL certificate to FortiClient EMS for Chromebooks.
	SSL certificate not from a common CA	• Add SSL certificate to FortiClient EMS for Chromebooks. • Add the root CA of your certificate to Google Admin console.
Allow FortiClient Chromebook Web Filter extension to trust FortiAnalyzer for logging	Public SSL certificate	• Add SSL certificate to FortiAnalyzer.
	SSL certificate not from a common CA	• Add SSL certificate to FortiAnalyzer. • Add the root CA of your certificate to Google Admin console.

Adding root certificates to Google Admin console

To add root certificates:

1. In Google Admin console, go to *Device Management* > *Network* > *Certificates (root certificate) (crt certificate)*.
2. Add the root certificate.
3. Select the *Use this certificate as an HTTPS certificate authority* check box.

Do not forget to select the *Use this certificate as an HTTPS certificate authority* check box.



Disallowing incognito mode

When users browse in incognito mode, extensions will be bypassed. Incognito mode should be disallowed for managed Google domains.

To disallow incognito mode:

1. In Google Admin console, go to *Device management* > *Chrome management* > *User settings*.
2. On the left, select the organization.
3. In the *Security* section, set *Incognito Mode* to *Disallow incognito mode*.
4. Click *Save*.

Service Account Credentials Setup

FortiClient EMS for Chromebooks requires Service Account Credentials generated by the Google Developer console. You can use the default Service Account Credentials provided with FortiClient EMS for Chromebooks, or you can generate and use unique Service Account Credentials, which is more secure.

This section describes how to configure default and unique Service Account Credentials. See the following sections:

- Configuring default Service Account Credentials on page 17
- Configuring unique Service Account Credentials on page 18

The Service Account Credentials must be the same in FortiClient EMS for Chromebooks and Google Admin console.

Configuring default Service Account Credentials

FortiClient EMS for Chromebooks includes the following default Service Account Credentials generated by the Google Developer console:

Option	Default Setting	Where Used
Client ID	102515977741391213738	Google Admin console
Service Account ID (Email address)	account-1@forticli-entwebfilter.iam.gserviceaccount.com	FortiClient EMS for Chromebooks
Service Account Certificate	A certificate in `.pem` format for the Service Account Credentials	FortiClient EMS for Chromebooks

The Service Account Credentials are a set. If you change one of the credentials, you must also change the other two credentials.

Adding the default Service Account Client ED in Google Admin console

To configure the default Service Account Credentials, you must add the default value for the Client ID to Google Admin Console. No other configuration for Service Account Credentials is required. See Adding Service Account Credentials to Google Admin console on page 18.

Configuring unique Service Account Credentials

When using unique Service Account Credentials for improved security, you must complete the following steps to add the unique Service Account Credentials to Google Admin console and FortiClient EMS for Chromebooks:

1. Create unique Service Account Credentials by using Google Developer console. See Creating unique Service Account Credentials on page 18
2. Add the unique Service Account Credentials to Google Admin console. See Adding Service Account Credentials to Google Admin console on page 18.
3. Add the unique Service Account Credentials to FortiClient EMS for Chromebooks. See Adding Service Account Credentials to FortiClient EMS for Chromebooks on page 18.

Creating unique Service Account Credentials

Use Google Developer console to create unique Service Account Credentials. For details, see the *FortiClient EMS for Chromebooks Administration Guide*. Unique Service Account Credentials include the following:

- Client ID (a long number)
- Service Account ID (Email address)
- Service Account Certificate (a certificate in `.pem` format)

Adding Service Account Credentials to Google Admin console

This section describes how to add the Client ID from the Service Account Credentials to Google Admin console. These settings allow Google to trust FortiClient EMS for Chromebooks, which enables FortiClient EMS for Chromebooks to retrieve information from the Google domain.

To add the Client ID:

1. In Google Admin console, go to *Security* > *Advanced settings* > *(you might need to click "show more" to see this)* > *Manage API client access*.
2. Set the following options:
   a. For the *Client Name* option, add the Client ID, which is a long number, from the Server Account Credentials.
   b. For the *API Scopes* option, copy and paste the following string:
   https://www.googleapis.com/auth/admin.directory.orgunit.readonly,https://www.googleapis.com/auth/admin.directory.user.readonly

The API Scopes are case-sensitive and must be lowercase. You might need to copy the string into a text editor and remove spaces created by words wrapping to the second line in the PDF.

3. Click *Authorize*.

Adding Service Account Credentials to FortiClient EMS for Chromebooks

The section describes how to add the Service Account ID and the Service Account Certificate from the Service Account Credentials to FortiClient EMS for Chromebooks.

To add Service Account Credentials:

1. In FortiClient EMS for Chromebooks, go to *View* > *Settings*.
2. Click *EMS for Chromebook*, and set the following options:

The default Service Account ID is displayed. Overwrite the default settings with the unique set of Service Account Credentials that you received from Fortinet.

New Service Account ID	Type the email address provided with the Service Account Credentials.
New Service Account Key	Click *Browse*, and select the certificate provided with the Service Account Credentials.

3. Click *Save*.

FortiClient EMS for Chromebooks Setup

This section describes how to set up FortiClient EMS for Chromebooks. Following is a summary of how to set up FortiClient EMS for Chromebooks:

1. Add an SSL certificate. See Adding SSL certificates on page 20.
2. Add the Google domain. See Adding the Google domain on page 21.
3. Create an endpoint profile. See Creating endpoint profiles on page 21.
4. Assign the endpoint profile to the Google domain. See Assigning endpoint profiles to domains on page 22.

Adding SSL certificates

This section includes the following procedures:

- Required: Adding SSL certificates to FortiClient EMS for Chromebooks on page 20
- Required only when sending logs to FortiAnalyzer: Adding SSL certificates to FortiAnalyzer on page 20

Adding SSL certificates to FortiClient EMS for Chromebooks

You must add an SSL certificate to FortiClient EMS for Chromebooks to allow HTTPS connections with Google Admin console.

If you are using a public SSL certificate, add the certificate to FortiClient EMS for Chromebooks. You do not need to add the certificate to Google Admin console.

If you are not using a public SSL certificate, you must add the SSL certificate to FortiClient EMS for Chromebooks, and you must add the root certificate to Google Admin console. See Adding root certificates on page 14.

To add SSL certificates to FortiClient EMS for Chromebooks:

1. In FortiClient EMS, go to *View >Settings*.
2. Click the *EMS for Chromebook*.
3. Beside *New SSL Certificate File*, click *Browse*, and locate the certificate file (server.pfx) and its password.
4. Click *Save*.

Adding SSL certificates to FortiAnalyzer

This section applies only if you're sending logs to FortiAnalyzer. If you're not sending logs to FortiAnalyzer, you can skip this section.

Sending logs to FortiAnalyzer requires that you add FortiClient EMS for Chromebooks to FortiAnalyzer. FortiClient EMS for Chromebooks is added as a device to the FortiClient ADOM in FortiAnalyzer. For information on adding a device to FortiAnalyzer, see the *FortiAnalyzer Administration Guide*.

An HTTPS connection is required to support logging from FortiClient EMS for Chromebooks to FortiAnalyzer, and you must set up an SSL certificate to support the HTTPS connection.

If you are using a public SSL certificate, add the certificate to FortiAnalyzer. You do not need to add the certificate to Google Admin console.

If you are not using a public SSL certificate, you must add the SSL certificate to FortiAnalyzer, and you must add the root certificate to Google Admin console. See Adding root certificates on page 14.

The common name of the certificate must be the IP address of your FortiAnalyzer.

To add SSL certificates to FortiAnalyzer:

1. In FortiAnalyzer, go to *System Settings* > *Certificates* > *Local Certificates*.
2. Click *Import*. The *Import Local Certificate* dialog box is displayed.
3. In the *Type* list, select *Certificate*.
   Or, in the *Type* list, select *PKCS #12 Certificate* to upload the certificate in PK12 format.
4. Beside *Certificate File*, click *Browse* to select the certificate.
5. Enter the password and certificate name.
6. Click *OK*.

To select certificates for HTTPS connections:

1. In FortiAnalyzer, go to *System Settings* > *Admin* > *Admin Settings*.
2. In the *HTTPS & Web Service Certificate* box, select the certificate that you want to use for HTTPS connections, and click *Apply*.

Adding the Google domain

To add the Google domain:

1. In FortiClient EMS for Chromebooks, in the *Google Domains* area, click the *Add a new Google domain* icon.
2. In the *Domain Admin Email* box, type your Google domain admin email, and type the *Domain Organization Unit Path*.

The forward slash (/) in the *Domain Organization Unit Path* box stands for the root of the domain.

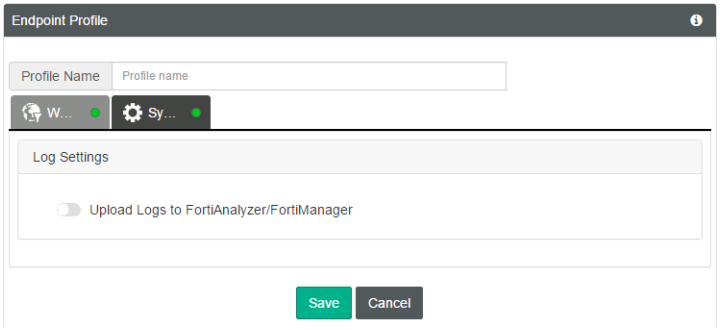
3. Click *Add Domain*.
   The Google domain information and users are imported into FortiClient EMS for Chromebooks.

Creating endpoint profiles

You can use the default endpoint profile, or you can create one or more endpoint profiles.

To create endpoint profiles:

1. From the *Endpoint Profiles* pane toolbar, click *Add a new profile*. The *Endpoint Profile* pane opens.
   Alternately, you can click the *Clone* icon in the default profile row to create a new endpoint profile based on the default endpoint profile.



2. In the *Profile Name* box, type a name for the profile.
3. Configure the options on the *Web Filter* and *System Settings* tabs.
   For a description of the options, see the *FortiClient EMS for Chromebooks Administration Guide*.
4. Click *Save* to save the endpoint profile.

Assigning endpoint profiles to domains

After creating the endpoint profile, you can apply the endpoint profile to domains or sub organizational units by using the right-click menu. If you do not apply an endpoint profile to a specific domain, the default endpoint profile is automatically applied.

After the endpoint profile is assigned to domain(s), FortiClient EMS for Chromebooks deploys the profile to Chromebook endpoints.

To assign endpoint profiles:

1. Go to *Domains*.
2. Right-click a domain or sub organizational unit, select *Assign Profile*, and then the profile. The profile is assigned.

FORTINET®

High Performance Network Security